

Project: DRA FRONT END FILTER PROJECT

Title: Project Overview Document

Ref: DS/FMU/FEF/001 *Issue:* 1.26 *Date:* 16 February 1994

Status: Approved *Type:* Project Overview

Keywords:

Author:

<i>Name</i>	<i>Location</i>	<i>Signature</i>	<i>Date</i>
G. M. Prout	WIN01		

Authorisation for Issue:

<i>Name</i>	<i>Function</i>	<i>Signature</i>	<i>Date</i>
R. B. Jones	HAT Manager		

Abstract: This document gives an overview of the documentation structure and the quality procedures for the DRA front end filter project RSRE 1C/6130.

Distribution: HAT FEF File

0 DOCUMENT CONTROL

0.1 Contents List

0	DOCUMENT CONTROL	2
0.1	Contents List	2
0.2	Document Cross References	4
0.3	Changes History	4
0.4	Changes Forecast	4
1	GENERAL	5
1.1	Scope	5
1.2	Introduction	5
1.3	Terminology	5
2	PROOFPOWER	5
3	CONFIGURATION MANAGEMENT AND CHANGE CONTROL	6
3.1	Hardware and Operating System	6
3.2	Source Code Control System SCCS	6
4	DIRECTORY STRUCTURE	6
5	DOCUMENT SUMMARIES	7
5.1	001 Project Overview Document	7
5.2	002 Errors in the SSQL Specification	7
5.3	003 Formal Security Policy	7
5.4	004 Specification of SSQL Semantics I	7
5.5	005 Specifications of <i>hide</i> and <i>updateState</i>	7
5.6	006 Security Conjectures for the SSQL Abstract Machine	7
5.7	007 Proof Strategy	7
5.8	008 Index of Theories	7
5.9	009 Proof of Security (I)	8
5.10	010 Proof of Security (IIa)	8
5.11	011 Proof of Security (IIb)	8
5.12	012 Proof of Security (IIc)	8
5.13	013 Proof of Security (IId)	8
5.14	014 Specification of SSQL Semantics II	8
5.15	015 Proof of Security (IIe)	8
5.16	016 Informal Justifications for Proof of Security	8
5.17	017 ProofPower Theory Listings	9
5.18	018 Proposal for Phase 2	9
5.19	019 Specification of Query Transformations in SML (I)	9
5.20	020 Specification of Query Transformations in SML (II)	9
5.21	021 Specification of TSQL	9
5.22	022 SWORD Front End Architectural Model	9
5.23	023 A Standard ML Specification of the Output Filter	9
5.24	024 A HOL Specification of the SWORD Output Filter	9
5.25	025 Representation of an SSQL State as a TSQL State	9

5.26	026	Critical Requirements on the SWORD Query Transformations	9
5.27	027	Representation of an SSQL State as a Derived Table	10
5.28	028	Specification of Query Transformations in HOL (I)	10
5.29	029	Specification of Query Transformations in HOL (II)	10
5.30	030	Presentation on FEF Phase I	10
5.31	031	Execution Model Security Proofs	10
5.32	032	Table Computations for SWORD	10
5.33	033	Value Computation Security Proofs	10
5.34	034	Phase II Proof Strategy	10
5.35	035	Table Computation Security Proofs	10
5.36	036	Phase II Proof Finale	10
5.37	037	Implementation for FEF Makefile	11
5.38	038	Architectural Model Security Proofs	11
5.39	039	Proposal and Quotation for Phase 3	11
5.40	040	Multi-level Formal Security Policy	11
5.41	041	Briefing for CLEF	11
5.42	042	Multi-Level Architectural Model	11
5.43	043	The Labelling Property for SWORD	11
5.44	044	Proofs About Labelling	11
5.45	045	Phase 3 Theory Listings	11
5.46	046	Technical Overview and Final Report	11
5.47	047	FEF Project Final Report	12
5.48	048	Report on Phase 3 Proofs	12
6		PHASE 1 DELIVERABLES	13
7		PHASE 2 DELIVERABLES	14
8		PHASE 3 DELIVERABLES	14
9		DOCUMENT PREPARATION	14
10		SCHEDULE FOR BACKING UP THE <i>fef</i> USERNAME	15

List of Tables

1	Project Directory Structure	6
2	Phase 1 Deliverables	13
3	Additional Phase 1 Documents	13
4	Phase 2 Deliverables	14
5	Deliverables for Phase 3	14

0.2 Document Cross References

- [1] *Secure Database Technical Proposal - Amendent 1*. High Assurance Team, ICL Secure Systems, WIN01, 11th February 1992.
- [2] *Secure Database Technical Proposal - Amendent 2*. High Assurance Team, ICL Secure Systems, WIN01, 22nd July 1992.
- [3] DS/FMU/017. *Secure Database Technical Proposal*. High Assurance Team, ICL Secure Systems, WIN01, 21st January 1992.
- [4] DS/FMU/FEF/018. *Proposal for Phase 2*. G.M. Prout, ICL Secure Systems, WIN01.
- [5] DS/FMU/FEF/022. *SWORD Front End Architectural Model*. R.D. Arthan, ICL Secure Systems, WIN01.
- [6] DS/FMU/FEF/026. *Critical Requirements on the SWORD Query Transformations*. R.D. Arthan, ICL Secure Systems, WIN01.
- [7] DS/FMU/FEF/031. *Execution Model Security Proofs*. R.D. Arthan, ICL Secure Systems, WIN01.
- [8] DS/FMU/FEF/032. *Table Computations for SWORD*. R.D. Arthan, ICL Secure Systems, WIN01.
- [9] DS/FMU/FEF/039. *Proposal and Quotation for Phase 3*. R.D. Arthan, ICL Secure Systems, WIN01.
- [10] DS/FMU/IED/USR006. *ProofPower Reference Manual*. Lemma 1 Ltd., <http://www.lemma-one.com>.
- [11] *SunOS Release 4.1 Documentation*. Sun Microsystems, Inc.
- [12] tp.qwg.001. *TP Quality Guide*. R.B. Jones, ICL Secure Systems, <http://www.lemma-one.com>.
- [13] tp.qwg.002. *TP Documentation Standard*. A.W. Walton, ICL Secure Systems, <http://www.lemma-one.com>.

0.3 Changes History

Issue 2.2 Removed dependency on ICL font.

0.4 Changes Forecast

1 GENERAL

1.1 Scope

This document identifies the quality procedures to be adhered to in the DRA front end filter project RSRE 1C/6130. This document also defines the configuration management practices to be followed for the DRA front end filter project RSRE 1C/6130. This is intended to cover all documentation and formal texts.

1.2 Introduction

This document acts as an overview to the DRA front end filter project. It describes the directory structure for the project filestore and gives a list of the documents in the project together with brief abstracts of their contents. The quality control mechanisms for the project are defined in the suite of documents referred to in the ICL Technology Projects Quality Guide, [12]. All the documents produced for this project to be delivered to the customer will conform to the standards defined in the Technology Projects Documentation Standards, [13], except that the final report may be in a format requested by the customer. The approval authority for deliverables to DRA is Roger Jones, the manager of the High Assurance Team (HAT). The main background document to the project is the original proposal, [3]. Amendments to the proposal may be found in [1] and [2].

The final section, 10, describes the procedure for backing up the *fef* username.

1.3 Terminology

literate script This is a file which contains both formal material (a program or a specification, say) and narrative text. The formal material can be automatically extracted for processing (e.g. by a compiler). The file can be typeset (using \LaTeX) to give a document standard listing of the formal material and the narrative. The formal material is held in the document in such a way that it can also be extracted fairly easily when using an interactive compiler or similar program.

2 PROOFPOWER

Reference is made throughout this document to the **ProofPower** system. This is the chosen theorem proving tool for this project, referred to in the original proposal, [3], as ICL HOL. The facilities available in **ProofPower** are documented in [10]

3 CONFIGURATION MANAGEMENT AND CHANGE CONTROL

3.1 Hardware and Operating System

The project is being carried out on Sun workstations networked via the Winnersh site LAN. The systems run Sun Microsystems' variant (SUNOS) of the UNIX operating system. The project is currently working with version 4.1.1 of this operating system.

For the purposes of this document the UNIX operating system will be taken to include the programs and the programming interfaces described in [11].

3.2 Source Code Control System SCCS

The UNIX configuration control system `sccs` will be the basic configuration control mechanism for the project. This document assumes familiarity with `sccs` (see [11]) and with the UNIX build control system `make`. All source files in the project library will be held under `sccs` control. They will be literate scripts prepared using \LaTeX supplemented by the features available in the `ProofPower` system for printing documents containing Z and HOL. All theories under the `ProofPower` system will be generated by such documents automatically using the facilities provided in the `ProofPower` system and the UNIX `make` facility. Documents should always contain an index of defining occurrences of formal names occurring in them, which should be the last section of the document. The penultimate section of all documents which create theories will usually be a listing of the theory.

4 DIRECTORY STRUCTURE

The definitive versions of all material prepared in the project on the SUN network is held in directories owned by the user `fef`. The master form for all documentation is held under `sccs` control in the filestore of the HAT SUN network in directories owned by the user `fef`. The directory structure of this user's home directory is described in table 1.

Name	Description
<code>~fef/SCCS</code>	<code>sccs</code> database directory for project documentation and related files.
<code>~fef/docs</code>	Used for preparation of documents other than literate scripts.
<code>~fef/build</code>	This directory will be used for building working versions of the theory structure. This directory will contain its own makefile, which may use more recent versions of documents than those in the 'approved' directory.
<code>~fef/tex</code>	Holds \TeX -ware which is specific to the project (e.g. the bibliography database <code>fef.bib</code>).

Table 1: Project Directory Structure

The home directory will also contain directories for holding general \TeX -ware and `ProofPower` software.

5 DOCUMENT SUMMARIES

This section gives a summary of the content of each document produced in the DRA front end filter project. Document references are of the form ‘DS/FMU/FEF/nnn’, where nnn is a three digit number. All documents are held under `sccs` control in the directory `~fef/SCCS`. The name of the `sccs` file is derived from the document reference, e.g. “DS/FMU/FEF/999” would be held in `~fef/SCCS/s.fef999.doc`.

5.1 001 Project Overview Document

This document [DS/FMU/FEF/001]

5.2 002 Errors in the SSQL Specification

A record of errors found in the SSQL specification, and changes made from Annex 2 of the ITT [DS/FMU/FEF/002]

5.3 003 Formal Security Policy

The formalisation of the security conjecture is in this document [DS/FMU/FEF/003]

5.4 004 Specification of SSQL Semantics I

The formal specifications of the main functionality of the SSQL semantics [DS/FMU/FEF/004]

5.5 005 Specifications of *hide* and *updateState*

The formal specifications of the functions *hide* and *updateState* [DS/FMU/FEF/005]

5.6 006 Security Conjectures for the SSQL Abstract Machine

The formal specification of the SSQL abstract machine and the conjecture to be proven in order to prove its security [DS/FMU/FEF/006]

5.7 007 Proof Strategy

A proof strategy for proving the conjecture of DS/FMU/FEF/005 [DS/FMU/FEF/007]

5.8 008 Index of Theories

A listing of all the constants, types and aliases, with their defining theories, that are available for use in the `fef` project [DS/FMU/FEF/008]

5.9 009 Proof of Security (I)

A formal proof of the unwinding result, part of the proof of security of the SSQL Abstract Machine[DS/FMU/FEF/009]

5.10 010 Proof of Security (IIa)

A formal proof of the security property on *hide*, part of the proof of security of the SSQL Abstract Machine[DS/FMU/FEF/010]

5.11 011 Proof of Security (IIb)

A formal proof conjuncts three and four of the security property on the relationship between *hide* and *updateState*, part of the proof of security of the SSQL Abstract Machine[DS/FMU/FEF/011]

5.12 012 Proof of Security (IIc)

A formal proof of conjunct one of the security property on the relationship between *hide* and *updateState*, part of the proof of security of the SSQL Abstract Machine[DS/FMU/FEF/012]

5.13 013 Proof of Security (IId)

A formal proof of conjunct two of the security property on the relationship between *hide* and *updateState*[DS/FMU/FEF/013]

5.14 014 Specification of SSQL Semantics II

The formal specification of the function *processQuery*. This completes the specification of the main functionality of the SSQL semantics [DS/FMU/FEF/014]

5.15 015 Proof of Security (IIe)

A formal proof that *updateState* maintains the invariant on the state. This result, together with the proofs from DS/FMU/FEF/011, DS/FMU/FEF/012 and DS/FMU/FEF/013, is used to prove the security property on the relationship between *hide* and *updateState*. This result in turn is used together with the proofs from DS/FMU/FEF/009 and DS/FMU/FEF/010 to complete the Phase 1 security proof, namely that $\vdash \text{behaviours } SSQLam \in \text{secure}$ [DS/FMU/FEF/015]

5.16 016 Informal Justifications for Proof of Security

Informal justifications of those axioms which have been included in the Phase 1 formal proof of security[DS/FMU/FEF/016]

5.17 017 ProofPower Theory Listings

Listings of all the ProofPower theories used in the DRA front end filter project [DS/FMU/FEF/017]

5.18 018 Proposal for Phase 2

The revised proposal for Phase 2 [DS/FMU/FEF/018]

5.19 019 Specification of Query Transformations in SML (I)

Standard ML functions and SSQL and TSQL datatype specifications required for the SSQL transformation specifications [DS/FMU/FEF/019]

5.20 020 Specification of Query Transformations in SML (II)

Specifications of the SSQL transformations in Standard ML [DS/FMU/FEF/020]

5.21 021 Specification of TSQL

Specifications of the TSQL abstract machine [DS/FMU/FEF/021]

5.22 022 SWORD Front End Architectural Model

Top level specifications of a model of the SWORD Front End [DS/FMU/FEF/022]

5.23 023 A Standard ML Specification of the Output Filter

A specification of the output filter in Standard ML for the SWORD Front End [DS/FMU/FEF/023]

5.24 024 A HOL Specification of the SWORD Output Filter

A ProofPower-HOL specification of the SWORD output filter [DS/FMU/FEF/024]

5.25 025 Representation of an SSQL State as a TSQL State

The formal specification of a mapping from an SSQL abstract machine state to the TSQL state which represents it [DS/FMU/FEF/025]

5.26 026 Critical Requirements on the SWORD Query Transformations

A ProofPower-HOL specification of the Critical Requirements on the SWORD Query Transformations [DS/FMU/FEF/026]

5.27 027 Representation of an SSQL State as a Derived Table

The formal specification of a mapping from an SSQL abstract machine state to a derived table as specified in fef026 [DS/FMU/FEF/027]

5.28 028 Specification of Query Transformations in HOL (I)

First part of the HOL specification of the SSQL transformation specifications [DS/FMU/FEF/023]

5.29 029 Specification of Query Transformations in HOL (II)

Second part of the HOL specification of the SSQL transformation specifications [DS/FMU/FEF/023]

5.30 030 Presentation on FEF Phase I

Slitex document containing overheads for FEF presentation.

5.31 031 Execution Model Security Proofs

Security proofs relating to the Execution Model of [6] [DS/FMU/FEF/031]

5.32 032 Table Computations for SWORD

Specifications of the computations which are allowed to be performed by the Execution Model of [7] [DS/FMU/FEF/032]

5.33 033 Value Computation Security Proofs

Security proofs relating to the value computations of [8] [DS/FMU/FEF/033]

5.34 034 Phase II Proof Strategy

The strategy for the Phase II proofs. [DS/FMU/FEF/034]

5.35 035 Table Computation Security Proofs

Security proofs relating to the table computations of [8] [DS/FMU/FEF/035]

5.36 036 Phase II Proof Finale

Incorporation of Table Computation Security Proofs and Execution Model Security Proofs into overall partial proof for Phase II [DS/FMU/FEF/036]

5.37 037 Implementation for FEF Makefile

A revised makefile for the project material [DS/FMU/FEF/037]

5.38 038 Architectural Model Security Proofs

Contains some proofs relating to the Architectural Model of [5] [DS/FMU/FEF/038]

5.39 039 Proposal and Quotation for Phase 3

A proposal for an extension to the scope of phase 3 of the project. [DS/FMU/FEF/039]

5.40 040 Multi-level Formal Security Policy

A formalisation of a multi-level version of the security policy. [DS/FMU/FEF/040]

5.41 041 Briefing for CLEF

A briefing suitable for a CLEF on the FEF work. [DS/FMU/FEF/041]

5.42 042 Multi-Level Architectural Model

A formulation of a somewhat simplified model of the multi-level SWORD database. [DS/FMU/FEF/042]

5.43 043 The Labelling Property for SWORD

A discussion and formalisation of an abstract 'labelling property' for SWORD. [DS/FMU/FEF/044]

5.44 044 Proofs About Labelling

Formal proofs establishing various results about the multi-level policy and the labelling property for SWORD. [DS/FMU/FEF/044]

5.45 045 Phase 3 Theory Listings

This document contains listings of the theories developed under Pphase 3 of the FEF contract, together with an index. [DS/FMU/FEF/045]

5.46 046 Technical Overview and Final Report

This document gives an overview of the formal work carried out under the phase 3 of the FEF project and serves as the final report on that work. It also discusses the relationship between the phase 2 and phase 3 work and suggests some possible directions for future research. [DS/FMU/FEF/046]

5.47 047 FEF Project Final Report

A final report on all aspects of the FEF contract. [DS/FMU/FEF/047]

5.48 048 Report on Phase 3 Proofs

A report on the proof work carried out in phase 3. [DS/FMU/FEF/048]

6 PHASE 1 DELIVERABLES

In this section we include the table of deliverables from [3], [1] and [2], together with the name and delivery date of the latest version of documents delivered.

WP	Code	Description	Draft	Final	Document	Sent
WP1a	D1	Formal Security Policy	wk1	wk3	fef003 v5.1	08/12
WP1a	D2	Specifications of 'hide' and 'update'	wk3	wk15	fef005 v4.1	08/12
WP1a	D3	Specifications of SSQL semantics I	wk22	wk30	fef004 v4.1	08/12
WP1a	D3	Specifications of SSQL semantics II	wk22	wk30	fef014 v2.1	08/12
WP1a	D4	Specification of security conjecture	wk6	wk12	fef006 v4.1	08/12
WP1b	D5	Unwinding proof scripts	-	wk18	fef009 v3.1	08/12
WP1b	D16	Informal justification for unwinding proof	-	wk18	fef009 v3.1	08/12
WP1c	D6	Remaining proof scripts	-	wk39	fef010 v2.1	08/12
			-	wk39	fef011 v2.1	08/12
			-	wk39	fef012 v2.1	08/12
			-	wk39	fef013 v2.1	08/12
			-	wk39	fef015 v2.1	08/12
WP1c	D17	Informal justifications for remaining proof	wk35	wk39	fef016 v2.1	08/12
WP2	D7	Proposal for Phase 2	-	wk39	fef018 v1.9	5/1/93

Table 2: Phase 1 Deliverables

The following have also been delivered to DRA:

Description	Document	Sent
Proof Strategy	fef007 v2.1	08/12
Cross Reference Index	fef008 v3.1	08/12
ProofPower Theory Listings	fef017 v2.1	08/12

Table 3: Additional Phase 1 Documents

7 PHASE 2 DELIVERABLES

In this section we include the table of deliverables from [4] as amended and agreed according to a letter to DRA of 6/1/93 (ref. fef/letters/dra9), together with the description and delivery date of the material to be delivered.

WP	Code	Description	Draft	Final
WP3	D8	Query Transformation Specifications in SML	wk6	wk8
WP3	D9	TSQL abstract machine specifications	wk18	wk50
WP3	D10	Query Transformation Specifications in HOL	wk6	wk50
WP3	D11	SSQL Implementation Model Specifications	wk18	wk50
WP3	D12	Specification of Security Propositions	wk34	wk50
WP3	D13	Phase 2 Proof Scripts	-	wk50
WP4	D14	Report on Phase 2 Proofs	-	wk50

Table 4: Phase 2 Deliverables

8 PHASE 3 DELIVERABLES

The deliverables for the extended phase 3 as described in [9] are listed in table 5.

WP	Code	Description	Draft	Final
WP7a	D15	Managerial Final Report	wk7	wk10
WP7b	D16	CLEF Report	wk4	wk6
WP7c	D17	Formal specification of non-interference and result-labelling property for multi-level objects	wk7	wk10
WP7d	D18	Report on consistency and other proof opportunities	-	wk10
WP7e	D19	Report on relationship between phase 2 and phase 3 treatments	-	wk10

Table 5: Deliverables for Phase 3

9 DOCUMENT PREPARATION

All the documents for this project, apart perhaps for the final report, will conform to the standards defined in TP.QWG.002. When a document has passed all inspections prior to internal approval it will then be printed with its correct issue number. Authorised issues will normally have issue numbers of the form 'n.1'.

All documents containing formal text will be printed with an index which will contain as a minimum the defining occurrences of all the formally defined names.

All documents which create a theory will usually contain a listing of the theory.

10 SCHEDULE FOR BACKING UP THE *fef* USERNAME

The definitive SCCS for *fef* is in the *fef* user held on Quine. This is covered by the standard backup procedures for that network.